Sub a1

WE CLAIM:

1. A disk drive 2 comprising:

(a) a disk 4 for storing data, the disk 4 comprising a public area 6 for storing plaintext data and a pristine area 8 for storing encrypted data;

(b) a head 10 for reading the encrypted data from the pristine area 8 of the disk 4;

(c) a control system 12 for controlling access to the pristine area 8 of the disk 4;

(d) authentication circuitry 14 for authenticating a request received from an external entity to access the pristine area 8 of the disk 4 and for enabling the control system 12 if the request is authenticated;

(e) a secret drive key 16; and

(f) decryption circuitry 18, responsive to the secret drive key 16, for decrypting the encrypted data stored in the pristine area 8 of the disk 4 to generate decrypted data.

2. The disk drive of claim 1, wherein the encrypted data comprises encrypted authentication data.

3. The disk drive of claim 2, wherein the authentication circuitry is responsive to the decrypted data.

4. The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted user authentication data.

5. The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted device authentication data for authenticating a device, the device comprising a unique device ID configured during manufacture of the device.

6. The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted

information for implementing a challenge and response verification sequence.

7. The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted message authentication data.

8. The disk drive of claim 7, wherein the encrypted authentication data comprises encrypted key data for generating a message authentication code.

9. The disk drive of claim 1, wherein the encrypted data comprises encrypted key data for decrypting an encrypted message.

10. The disk drive of claim 1, wherein the encrypted data comprises encrypted message data.

11. The disk drive of claim 1, wherein the disk drive further comprises encryption circuitry for encrypting plaintext data into the encrypted data stored in the pristine area.

12. The disk drive of claim 1, wherein:
(a) the disk further comprises embedded servo sectors comprising servo bursts;
(b) the control system comprises a servo control system responsive to the embedded servo sectors; and
(c) the authentication circuitry enables the servo control system.

13. The disk drive of claim 12, wherein:
(a) the servo bursts are written to the disk in encrypted form; and
(b) the authentication circuitry enables the servo control system to decrypt the servo bursts.

14. The disk drive of claim 13, wherein:

(a) the servo bursts are written to the disk with additive noise generated from a pseudo random sequence;

(b) the pseudo random sequence is generated from a polynomial;

(c) the servo control system uses the polynomial to decrypt the servo bursts; and

(d) the authentication circuitry provides the polynomial to the servo control system.

15. A disk drive comprising:

(a) a disk for storing data, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data;

(b) a head for reading data from the disk;

(c) a control system for controlling access to the disk;

(d) a secret drive key;

(e) decryption circuitry, responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area of the disk to generate decrypted data; and

(f) authentication circuitry, responsive to the decrypted data, for authenticating a request received from an external entity to access the disk and for enabling the control system if the request is authenticated.

16. A disk drive 2 comprising:

(a) a disk 4 for storing data, the disk 4 comprising a public area 6 for storing plaintext data and a pristine area 8 for storing encrypted data;

(b) a head 10 for reading the encrypted data from the pristine area 8 of the disk 4;

(c) a control system 12 for controlling access to the pristine area 8 of the disk 4;

(d) a secret drive key 16; and

(e) decryption circuitry 18, responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area 6 of the disk 4,

wherein:

the disk 4 comprises a plurality of physical blocks accessed by the control system through physical block addresses;

a request received from an external entity during normal operation of the disk drive comprises a logical block address which is mapped by the control system to a selected one of the physical block addresses; and

the pristine area comprises at least one physical block written with at least part of the encrypted data during manufacturing of the disk drive and not externally accessible through a logical block address during normal operation of the disk drive.

17. A method of processing a request received by a disk drive from an external entity to access encrypted data stored in a pristine area of a disk, the method comprising the steps of:

(a) authenticating the request to access the pristine area and enabling access to the pristine area if the request is authenticated;

(b) reading the encrypted data stored in the pristine area; and

(c) decrypting the encrypted data using a secret drive key within the disk drive to generate decrypted data.

18. The method as recited in claim 17, wherein the encrypted data comprises encrypted authentication data.

19. The method as recited in claim 18, wherein the step of authenticating is responsive to the decrypted data.

20. The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted user authentication data.

21. The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted device authentication data for authenticating a device, the device comprising a unique device ID configured during manufacture of the device.

22. The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted information for implementing a challenge and response verification sequence.

23. The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted message authentication data.

24. The method as recited in claim 23, wherein the encrypted authentication data comprises encrypted key data for generating a message authentication code.

25. The method as recited in claim 17, wherein the encrypted data comprises encrypted key data for decrypting an encrypted message.

26. The method as recited in claim 17, wherein the encrypted data comprises encrypted message data.

27. The method as recited in claim 17, further comprising the step of encrypting plaintext data to generate the encrypted data stored in the pristine area.

28. The method as recited in claim 17, wherein the disk further comprises embedded servo sectors comprising servo bursts, the method further comprising the steps of:
(a) servoing a head over the disk in response to the embedded servo sectors; and
(b) enabling servoing in the pristine area if the request is authenticated.

29. The disk drive of claim 28, wherein:
(a) the servo bursts are written to the disk in encrypted form; and
(b) the step of authenticating the request to access the pristine area comprises the step of decrypting the servo bursts.

30. The disk drive of claim 29, wherein:
(a) the servo bursts are written to the disk with additive noise generated from a pseudo random sequence;
(b) the pseudo random sequence is generated from a polynomial; and

(c) the step of servoing uses the polynomial to decrypt the servo bursts.

31. A method of processing a request received by a disk drive from an external entity to access data stored on a disk, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data, the method comprising the steps of:

(a) decrypting the encrypted data stored in the pristine area of the disk using a secret drive key within the disk drive to generate decrypted data; and

(b) using the decrypted data to authenticate the request received from the external entity before allowing access to the disk.